What Is the Future of European Cyber Security? Three Principles of European Cooperation and the Hybrid Joint Strategy of Cyber Defence

Samonek, Aleksandra

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:
Samonek, A. (2020). What Is the Future of European Cyber Security? Three Principles of European Cooperation and the Hybrid Joint Strategy of Cyber Defence. *Studia Europejskie - Studies in European Affairs*, *24*(2), 43-60. https://doi.org/10.33067/SE.2.2020.3

DOI: 10.33067/SE.2.2020.3

Aleksandra Samonek[★]

What Is the Future of European Cyber Security? Three Principles of European Cooperation and the Hybrid Joint Strategy of Cyber Defence

Abstract

The author argues that EU member states should pursue a joint strategy of cyber security and cyber defence. This claim does not immediately imply support for current EU legislation, in particular for enforcing the NIS Directive or the operation of ENISA in its currently planned capacity. Instead, three principles of European cooperation are discussed and followed by a proposal to centre the joint strategic effort around promoting and explicating the practical and procedural consequences of these principles. A bottom-up approach to joining and uniformization of European cyber defence is presented, aligned with the notion of Europeanization in security policy in the sense of E. Gross and R. Ladrech. This approach requires that European cyber security agencies, including ENISA, focus their efforts on addressing the trust deficit among the member states through facilitating the environment for safe information exchange, instead of communicating with the member states through the medium of regulations and prescribing security standards. More generally, the author postulates that the European authorities embrace the inherent political character of international trust-building and aspire to the role of mediator, as opposed to presenting themselves as apolitical agents focused on the purely technical aspects of European cyber security.

Keywords: European Policy, Cyber Security, European Single Market, European Cooperation

★ **Aleksandra Samonek** – Université Catholique de Louvain (UCLouvain) and Jagiellonian University, e-mail: aleksandra.samonek@uclouvain.be, ORCID: 0000-0002-5742-7190.

Introduction

In this paper three principles of European cooperation are isolated and discussed in the context of EU cyber security strategy, that is the principle of effectiveness, the principle of non-aggression and the principle of priority of the European Single Market (ESM). The first principle originates from the fact that the European nation states are jointly vulnerable to trans-border cyber threats. Ahead of the predicted increase in the adversarial activity of the nation state actors ahead of the 2020 Brexit transition and considering the substantial technological resources available to the attackers due to the trickling down effect,[1] the joint vulnerability of the EU members becomes all the more evident. In these circumstances, joining efforts in preventing the emerging threats is not only more efficient when it comes to risk and resources, but may turn out to be strategically necessary. The principle of non-aggression lies at the heart of the European project and expresses the directed efforts to solidify within the EU borders the 'miraculous change' in the nature of political international order, no longer dominated by the threat of military conflict.[2] Since the emergence of new forms of warfare, Europe has faced the need to redefine what it means for the EU nation states to maintain peace. Based on these readjusted peace conditions, a new and rather problematic meaning of non-aggression presents itself. Lastly, the priority of the ESM is visible not only in the magnitude of constitutive regulations, but also in clear declarations on the side of the European Commission that the ESM is to be treated as 'one of the EU's greatest achievements'.[3] As the external threats and country-specific vulnerabilities threaten the EU internal market integration through targeted attacks and the spillover effect, the priority of the ESM necessitates new measures in coordinating cyber security defense across the EU. The author will argue that these principles together shape the direction of development of the cyber security strategy at the EU level and help explain the current arrangement in the European joint cyber defense system.

First, some general characteristics of high-level (national or supernational) cyber defense are presented, focusing on the divergence between the notions of a cyber threat and cyber attack. This difference translates

[1] S. Curry, *How geopolitical events will change cybersecurity in 2020*, "Cybereason", December 19, 2019, https://www.cybereason.com/blog/how-geopolitical-events-will-change-cybersecurity-in-2020 (access 30.12.2019).

[2] P. Hassner, *An overview of the problem*, in: *War and Peace: European Conflict Prevention*, Chaillot Paper 11, Institute for Security Studies of WEU, 1993, p. 6.

[3] https://ec.europa.eu/growth/single-market_en (access 10.01.2020).

directly into the strategies of cyber defense in that a low-risk cyber defense strategy must be preventative in nature, as opposed to reactive, especially in application to a system protecting critical infrastructure of national or federal scope. Next, the European joint cyber defense system is presented as a hybrid created as a means of mitigating the expected negative consequences of maintaining a joint defense strategy *simpliciter* and separating the pan-European strategy into national cyber security programs. These considerations yield a suggestion of what a joint defense program in the current diplomatic and institutional setup entails for the EU members. An exposition of the three working principles of European cooperation follows, together with a discussion about their limitations in the context of EU cyber security. The image of the European cyber defense system arising from these deliberations is one-of-a-kind.

Preventative Strategies in High-level Cyber Defense Systems

At the very minimum, a cyber threat is understood as 'the possibility of a malicious attempt to damage or disrupt a computer network or system'.[4] This modest definition should be amended to include the possibility to access files and infiltrate or steal data, even in the absence of an attempt of damage or disruption.[5] In other words, the very possibility to put the network of a system in jeopardy constitutes a serious cyber threat. The latter version of an attack may potentially put the entire system of institutions relying on a secure channel of communication or database out of operation, simply by making the communication or data unreliable. One yet more important aspect of the proposed definition is that it correctly identifies a cyber threat as a possibility as opposed to an actual attack. An attack is merely one instance of a particular cyber threat, taking form of concrete actions against the security of information or the integrity of a network or a system.

The author will put aside the technological aspects of cyber attacks for the purposes of further considerations in favor of considering the strategies to combat cyber threats. The former are often of second-order importance to high-level defense policies, because there are not many known techniques available to deal with cyber attacks, other than through

[4] *Cyberthreat*, in: *Lexico (Oxford Dictionary)*, https://en.oxforddictionaries.com/definition/us/cyberthreat (access 25.05.2018).

[5] *Cyber Threat Basics, Types of Threats, Intelligence & Best Practices*, "Secureworks", May 12, 2017, https://www.secureworks.com/blog/cyber-threat-basics (access 25.05.2018).

prevention. In most scenarios knowledge about the attack is only gathered *ex post*. Consequently, most types of cyber attacks cannot be stopped or undone. The overwhelming impact of such attacks is visible in incidents like the Panama Papers case from 2016, where a simple unpatched software vulnerability was exploited,[6] or the Proton Mail Ransom case, where powerful distributed denial-of-service (DDoS) attacks were conducted, using resources available to very few actors, such as nation states or global business giants.[7] Once the possibility of an attack emerges and the door to exploitation of some vulnerability is forced open, there is close to nothing that a nation or a federation can do to avoid the consequences. Therefore, a high-level cyber security defense system aimed at maximizing security and minimizing risk is preventative in nature, rather than reactive. Insofar as the preventative measures of a high-level cyber security system belong in the defense agenda of the nation state or a federation, the reactive measures which are activated in case of an ongoing cyber attack, more often than not fall into the realms of crisis management and emergency strategies rather than align with any preexisting defense plan.

Another crucial feature of cyber security is that it contains in itself protection of persons and resources that benefit from the process of collecting and analyzing information.[8] Protecting information and communication is of great importance in any defense system, but ultimately information and communication safety is just a means of protecting other values and goods, as is clear in debates on, e.g., cyber terrorism. Thus, cyber security defense strategies protect what is instrumental to the operation and identity of the nation state or a federation, rather than simply protecting information and system security. This feature is especially prominent in high-level defense systems and can be called *instrumentality to protecting core values*.

Two Approaches to Cyber Defense in the EU

The EU member states carry the primary responsibility and competence to build and maintain their own national security systems. However, the EU has taken upon a project of building the Single Cybersecurity Market, a uniform system of security products, services and processes, which

[6] B. Obermayer, F. Obermaier, *The Panama Papers: Breaking the story of how the rich and powerful hide their money*, Oneworld Publications 2016, p. 339.

[7] S. Newman, *Surviving ransom driven DDoS extortion campaigns*, "Cyber Security: A Peer-Reviewed Journal", no. 3(1)/2019, pp. 38–39.

[8] R. Von Solms, J. Van Niekerk, *From information security to cyber security*, "Computers & Security", no. 38/2013, pp. 97–102.

among others shall protect the European market from a growing number of cyber threats.[9] The aim of the pan-European cyber security measures is to protect the European economy, especially the ESM, and the European democracy *via* eliminating the dispersion of fake news, misinformation campaigns and radicalization, and other relevant threats. These two types of systems – the EU Single Cybersecurity Market and general national security systems (national cyber security plans being their part) – are bound to come into conflict at many points related to cyber security, including issues such as the accepted certification frameworks, the level of investment in building a system of cyber defense and the prioritization in defense system design. Many of those problems are technical in nature and could, at least in principle, be solved by intensifying EU-national dialogue. However, certain other issues, which will be explored in more detail in what follows, are based on the trade-off of principles which differ across the member states and which are the source of fundamental conflicts between the national and pan-European cyber defense authorities.

As of today, the practical decisions concerning cyber security systems remain in the hands of nation states. However, a number of proposal for pan-European coordination have been put forth and at least partially introduced, initially in a top-down manner and with only symbolic consultations with the representatives of the member states. The existing measures of cyber protection which are at least partly implemented at the EU-level include:

i. the EU Cybersecurity Agency (formerly operating as the European Union Agency for Network and Information Security, or ENISA), which provides technical support and a consultancy for implementing of the EU cyber security regulations,
ii. the EU cyber security certification framework, intended to replace all national certification requirements,[10]
iii. the development of the EU Single Cybersecurity Market, with special attention to assessing the encryption of products and services used by citizens, businesses and governments within the Digital Single Market,
iv. the proposal to fully implement the Directive on the Security of Network and Information Systems in order to set higher standards for cyber security within the nation states.

[9] *Cf.* The joint communication to the European Parliament and the European Council of the European Commission's High Representative of the Union for Foreign Affairs and Security Policy "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", JOIN(2017) 450 final, Brussels, 13.09.2017.

[10] https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework (access 10.01.2020).

Some of the above measures met with resistance from the nation states. A permanent mandate for ENISA as well as the full implementation of the Directive on the Security of Network and Information Systems threatened to overhaul their national counterparts,[11] such as, in case of Germany, the CERT Alliance[12] and the cyber security strategy already in place. The initial reception of pan-European security measures was poor and not only in Germany. This lack of enthusiasm was part of the reason why the reforms mentioned in the joint communication from 2017 took exceedingly long time to set in motion. Although theoretically rebranded and with extended scope of competences, ENISA still operates partly under its original name and struggles for legitimacy among the security providers.[13] National security agencies operate in an almost unchanged manner and the only observable progress seems to happen within the legislation. One can reasonably expect that the EU plans for joint cyber security strategy will result in equal or greater amount of conflicts and objections than the program of unifying the laws concerning data protection, where several nation states simply missed the deadline for adopting the data protection laws complying with the EU objectives (initially set to May 25, 2018). The period of two years was insufficient for some of the EU members to adopt the EU uniform data protection regulations, including Belgium, Bulgaria, Cyprus, Czech Republic, Greece, Hungary, Lithuania and Slovenia.[14]

Meaningful lessons about the possible future development of the EU joint cyber security initiatives follow from observing the contention between Germany and the European Commission in the recent years, especially visible in the declarations of the representatives of the European Commission (representing also the EP and ENISA) and Germany's cyber security chief Arne Schönbohm. The conflict began with the cyber security solutions of the NIS Directive (Cybersecurity Directive),[15] which the European Parliament adopted on July 6, 2016 as the first EU-wide

[11] https://www.euractiv.com/section/cybersecurity/news/juncker-announces-massive-cyber-security-overhaul/ (access 10.03.2020).

[12] https://www.cert-verbund.de/ (access 25.05.2018).

[13] L. Brun, *The role of the European Union Agency for Network and Information Security (ENISA) in the governance strategies of European cybersecurity*, Faculté des sciences économiques, sociales, politiques et de communication, Université catholique de Louvain, Prom.: Bellanova, Rocco 2018, p. 7; K. Sliwinski, *Moving beyond the European Union's weakness as a cyber-security agent*, "Contemporary Security Policy", no. 35(3)/2014, pp. 468–486.

[14] https://euobserver.com/justice/141860 (access 10.03.2020).

[15] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, Brussels, 6.07.2016.

legislation concerning cyber security. The transposition deadline for the member states (May 9, 2018) met with instant opposition from some of the nation states, including Germany. After a period of diplomatic hurdles, the EU representatives agreed to respect national sovereignty in cyber security regulations and measures,[16] while Germany transposed a version of the NIS.[17] The points raised during the debate of 2017-2018 period included the following:[18]

1. The Commission attempted to overhaul the EU member's cyber security rules outside the proper partnership capacity and cooperation, and without building necessary trust in the member states;
2. The Commission failed to respect the relevant priorities and values of the member states, e.g. Germany's objective of making cyber security a *sine qua non* condition of digitization (while the EU institutions are inclined to pursue digitization even without proper cyber security measures) or the principle of mutual recognition (allowing various approaches to a given threat instead of a one-fit-all solution);
3. In case of Germany, the Commission tried to replace a more advanced security strategy with a less advanced one;
4. The Commission does not share with member states the information about the encryption technologies used to secure communications and other important aspects of its cyber security procedures, but requires the nation states to provide their encryption characteristics and comply with new standards, thus forcing centralization of decisions strategic to national defense;
5. The system of ranking the cyber security level of technology products is underdeveloped and, like other measures proposed by the Commission, weakens the regulations already existing in some nation states.

What is crucial here is that the UK and Germany developed strong cyber security units in their intelligence, security and military service prior to the joint EU cyber security initiative. Such national units, unlike any pan-European institution, including ENISA, may indeed have the capabilities necessary to prevent and discover certain types of advanced

[16] https://www.euractiv.com/section/cybersecurity/news/ansip-vows-to-respect-sovereignty-with-new-cybersecurity-measures/ (access 25.05.2018).

[17] https://ec.europa.eu/digital-single-market/en/implementation-nis-directive-germany (access 25.05.2018).

[18] https://www.euractiv.com/section/cybersecurity/interview/commission-should-walk-the-walk-on-cybersecurity-german-chief-says/ (access 25.05.2018); A talk at the EU Cyber Security Conference in Tallinn, October 23, 2017 by Arne Schönbohm and Guillaume Poupard, https://www.eu2017.ee/videos/eu-cyber-security-conference-arne-schonbohm-and-guillaume-poupard.html (access 25.05.2018).

cyber threats. From the purely financial perspective, the EU is unable to develop comparable defense systems. As Schönbohm noted, the EU authorities can provide consultation and advice, but they have nothing else to bring to the table.[19] However, even the member states whose cyber security defense systems are not as advanced as in Germany may find themselves facing similar issues as the ones exemplified in the German-EU conflict. In particular:

1. The EU members may have different priorities concerning cyber defense, for example, some EU members are willing to take the risk of digitalization despite a lack of proper cyber security measures and procedures because the value of economic growth driven by digitalization outgrows the estimated risks related to cyber threats, while others (like Germany or the UK) cannot afford to take the risk;
2. The EU members may be willing to contribute significantly different resources to cyber defense;
3. The EU institutions may prioritize different values than the nation states, for example, insist on protecting the right to privacy against government surveillance when the nation state finds such surveillance necessary or desirable;
4. A joint defense system means that a lot of information so far kept confidential by nation states will be made available to the European institutions, for example the characteristics of information collected, processed and protected by each member.

A more general underlying issue is that national security typically lies outside the EU competence, while IT security, mostly for the sake of developing Digital Single Market, is the focal point of EU digital cooperation. Considering these obstacles, can it still be expected that the EU members pursue a joint system of cyber security defense?

At first glance it seems that the separation of national cyber defense systems should make the nation states less vulnerable. The expected fallout of each attack would decrease if the consequences were limited to a single national system or a network and if the points of access were minimized. Accordingly, radical proposals of 'digital border control' across Europe emerged.[20] One of the weakest points in these proposals is that they aim to align the entire European cyber defense strategy so as to address cyber attacks and not cyber threats. In other words, such proposals equal postulating that the EU members adopt an overall

[19] Ibidem.

[20] https://www.euractiv.com/section/cybersecurity/news/europe-needs-digital-border-controls-industry-chief-says/ (access 3.03.2020).

reactive approach, instead of a preventative one (which follows, as was argued above, from centering the cyber security strategy around the consequences of attacks instead of preventing threats). Moreover, just as is the case with a physical security system, e.g. in military corps, uniting forces internationally allows nation states to raise the stakes for a potential adversary and intensify a potential retaliatory response. International cooperation allows for using human, organizational, economic, political and diplomatic resources which are simply unavailable to a single nation state.

From this point of view, the nation states with the weakest cyber security systems who do not have enough resources to maintain proper cyber defense should therefore be the most interested in joining forces with others. However, countries which may be put at risk *via* the spillover effect are also naturally interested in preventing threats to their physical or digital neighbors. Thus, from the most general perspective, joining the cyber security efforts across the EU primarily means that the member states aim to share the profits of well-functioning cyber security defense, together with sharing the financial burden as well as some of the related risks. For each nation state a pan-European cooperation would bring increased technical and financial capabilities, but also the need to comply with international agreements and mutual obligations which may prioritize different values than the ones of a nation state itself. What pursuing a joint defense strategy does not necessarily mean, however, is that the decisions concerning defense strategy are centralized or that the input of national security authorities should be reduced to executing the directives and decisions undertaken by the EU institutions.

Despite the fact that building a pan-European cyber defense system imitating national security system is not feasible, pursuing a joint defense strategy is still well within our reach. Rather than trying to scale up the already existing national defense strategies, the EU may facilitate a platform of exchanging and trading resources, know-how and skills between the national cyber security agencies. In other words, instead of creating a pan-European security agency – a project which is deemed to fail – the EU should aim to coordinate and enhance the work of national agencies and take the role of an advisor and mediator, instead of the legislator or an executive authority. The unification of national cyber defense system should therefore be voluntary and based on mutual trust, rather than on the obligation to transpose contentious legislation, which many EU members are likely to sabotage by impairing further development of solutions proposed in that legislation, as was the case with the operation of ENISA or shared systems of security evaluation.

Therefore, the author will argue for a bottom-up approach to European cyber security uniformity, rather than a top-down approach which seems to be pursued currently.

One might argue that since the top-down approach does not seem to be a working model for EU cooperation (for one, because of insufficient funds to develop pan-European agency with sufficient scope of competence without strong resistance from the member states), the European project of joint security strategy should be abandoned altogether. The main point of interest in this paper, however, is that despite its rough start and the need for major revisions, the project of a joint EU strategy of cyber defense is both needed and plausible. In what follows, three principles of European cooperation will be discussed, each independently motivating the joint cyber security efforts. The author will argue that if the three principles be prioritized in the EU cyber security strategy, the nation states will face a unique opportunity for trust-building and development. The strategy based on the prioritization of these principles is referred to as *hybrid*, as despite the clear joining of efforts it allows that the nation states protect crucial elements of their defense sovereignty.

Three Principles of European Cooperation

The Principle of Effectiveness

The fact that the EU members are jointly vulnerable to various cyber threats is vividly exemplified in the trans-border attacks which took place in the recent years, like the Wannacry attack[21] and the NotPetya attack from 2017,[22] the election campaign hacks in 2016 and 2017 where attacks were used to delegitimize the electoral process or cast a shadow over elected representatives.[23]

The expected future cyber threats concern the governmental (or otherwise public) information systems or networks, as well as the information systems of private agents operating on the territory of a given nation state. Both types of threats carry over to the national or European cyber defense systems. Accordingly, the German cyber security

[21] *Cf.* S. Ghafur, S. Kristensen, K. Honeyford, G. Martin, A. Darzi, P. Aylin, *A retrospective impact analysis of the WannaCry cyberattack on the NHS*, "NPJ digital medicine", no. *2*(1)/2019, pp. 1–7.

[22] E. Nakashima, *Russian military was behind NotPetya cyberattack in Ukraine, CIA concludes*, "The Washington Post", no. 12/2018; A. Greenberg, *The untold story of NotPetya, the most devastating cyberattack in history*, "Wired", August 22, 2018.

[23] M. Baezner, P. Robin, *Cyber-conflict between the United States of America and Russia* (No. 2), ETH Zurich 2017, p. 15.

cooperation group (the aforementioned CERT Alliance) is composed of over 40 private and public institutions which form a partnership based on voluntary participation and recognition of joint vulnerability rather than a hierarchical structure with governmental executive unit at the top.

Many of the companies involved in CERT Alliance are trans-national and operate on territories of other EU countries. The current situation where Germany attempts to protect the information systems of companies which operate also in other EU countries is suboptimal on multiple levels. First, in order to protect its information infrastructure and private market economy, Germany has to invest its resources in solutions which necessarily benefit all those countries which are under the operation of private companies included in German protection strategy. This creates imbalance, because some European countries become direct beneficiaries of the German cyber security system without contributing to it, effectively freeloading on the German approach to the safety of infrastructure. Conversely, in future, Germany may try to make up for its input into the economies of other EU members and demand diversification of business relationship of the companies and particular EU members. For example, in exchange for the protection against cyber threats, the companies may be required to offer better prices, products and services to consumers and institutions in Germany than in other EU countries. This direction of travel not only creates higher overall costs, but also weakens the ESM.

For certain countries which do not value its cyber defense as high as Germany, it might seem advantageous that the contributions to the cyber defense remain separate across the EU, as the counties heavily invested in information security will, as a side effect to their own agendas, protect parts of the digital economy of others. However, the investment in cyber security will sooner or later take visible effect on prices and service conditions offered to the freeloader. From the long-term perspective, such situations should be avoided for: first, the sake of fairness, second, due to the risk they pose to the freeloaders' participation in the ESM.

Despite the possibility to ease the imbalance of contributions, Germany is still promoting the idea of individual (national) protection against cyber threats. This is partly due to the fact that the current cyber security strategy in the EU impair the building of methods of balancing the contributions, either through legislation or voluntarily. Note that even Germany is not opposing the idea of trans-national cooperation in cyber defense, even at the pan-European level. Rather, it is opposing the approach which the European Commission takes as a default in promoting new cooperation methods. This approach includes passing on binding legislation which greatly exceeds technical issues and aims to

introduce uniformity among the member states by *averaging* the security requirements, instead of leveling up the quality of protection. Ultimately, adopting the default EU standards would mean that Germany is forced to keep up its financial responsibilities while having less control over its own security standards. Moreover, the common resistance towards ENISA often stems not from the lack of support to uniformity in the EU cyber security defense systems, but rather from justified fear of centralizing cyber security units in a way which is not in agreement with the EU members and without considering the alternative methods of pursuing a joint defense system. This fear could be partially done away with if the EU pursued its role as the *facilitator* (as opposed to the regulator) of the joint European cyber security efforts. The effectiveness principle suggests that, even in a situation when the nation states are reluctant to delegate decisions to the EU, they should be willing to take a seat at a negotiation table to lower their long-term costs (either direct, as in case of Germany, or indirect in case of those who will repay their lack of contribution in raised market prices for goods and services).

The Principle of Non-aggression

The non-aggression between the member states means lessening the possibility of war between the member states, understood both as a cyber war (mutual or one-sided attacks on information infrastructure) and as a regular war in which information security and safety of communication play a central role. Cyber threats constitute a vast catalog of potential hostile actions, including criminal, terrorist and hostile state-sponsored activity. A specific cyber threat may involve multiple such actions, which is why attributability problem occurs at two levels. First, it is nearly impossible to discover the identity of the attacker. Then again, without knowing the attacker's identity attributing motivation behind the attack is problematic. Cases of successful attributions are rare and mostly due to accidental leak or whistleblowing.[24] A typical cyber threat with far-reaching political and military consequences is the interception of communications. For instance, Welchman argued that breaking the enigma machine code by Bletchley Park cryptographers shortened the WWII by two whole years, and that Hitler's strategy of Blitzkrieg relied on safe communications in the battlefield.[25] Availability of safe communication is easily weaponized

[24] *Global intelligence oversight: governing security in the twenty-first century*, eds. Z. Goldman, S. Rascoff, Oxford University Press, Oxford 2016, p. 243.

[25] G. Welchman, *The Hut Six Story: Breaking the Enigma Codes*, M&M Baldwin, 1997, chapter 1.

and so it should be equally available to all the member states. This implies sharing critical protection standards and technologies across the EU.

Coming back to the identity attribution problem, the attackers may abuse third party resources to perform an attack, thus obscuring the source and leveraging third party ignorance against the system or network of interest. Oddly enough, unless the EU members commit their resources to building a joint defense strategy and facilitate the practice of sharing the information relevant to fending off the threats, it may become possible for one member state to be at war with another inadvertently *via* unwitting contribution of resources. One of the strongest motivations for the European project as a whole has been to avoid the war between the member states and preventing third party adversaries from leveraging the resources of one European country against the other.[26] Productive channels of sharing information and collective diagnosis of threats promise to extent this principle of pan-European non-aggression onto the field of security which emerged only after the conception of the European federation.

Understandably, sharing critical information often causes decision crises within national intelligence agencies. Building a joint cyber defense system cannot entail sharing all information with an unspecified and uncontrolled forum of European security personnel and members of all other national agencies. Therefore, addressing the *trust deficit* among the EU member states should have priority over all other goals of the joint European cyber security strategy. The already established coordination protocols for national security may be a good starting point. Namely, despite the fact that national military security remains outside the scope of the EU institutions and the decision outlets remain fully decentralized, European military strategies are not at all independent from each other. For one, the EU maintains the Common Security and Defence Policy (CSDP) to plan and respond to international crises.[27] If the joint cyber security system were to follow similar protocols, lack of a central cyber security agency would not be much of a problem, since separation of competence into nation states does not necessarily entail that the cyber security system cannot be coordinated and made uniform throughout the EU countries.

Then finally, the EU intelligence agencies do cooperate with each other on regular basis. What makes it hard to facilitate such cooperation in the context of pan-European relations is the perception of shifting

[26] J. Wouters, F. Naert, *The European Union and Conflict Prevention: a Brief Historic Overview*, "KULeuven Institut of International Law Working Paper", no. 52, April 2003, pp. 6–7.

[27] https://eeas.europa.eu/headquarters/headquarters-homepage/63376/stronger-eu-defence-face-global-challenges_en (access 10.12.2019).

the decisions concerning information exchange towards the top of the institutional hierarchy. If the EU were to facilitate the environment for safe information exchange instead of simply incentivizing the member states to reveal their intelligence materials, the project of joint cyber security strategy may bring one-of-a-kind value to European cooperation. By allowing the agencies to work together and helping build mutual trust between the EU members, the European institutions would contribute to both intensification of cyber security measures in the EU and further integration of the member states. In the current state of development of the EU cyber security strategy the trend is slowly shifting away from centralizing security units and enforcing regulations. However, this shift must be accelerated, and the European Cybersecurity Agenda modified so as to clearly serve the best interest of the member states.

The Principle of ESM Priority

The principle of ESM priority is perhaps the most self-evident of the three, as the large-scale business entities like Apple or Facebook tend to negotiate their policies and decisions almost exclusively with the European representatives, while rarely attempting to deal with the institutions of the member states. For instance, the European courts and EU data protection units have at their disposal powerful tools for changing the privacy policies, user agreements, invalidating patents and solutions which threaten to harm the EU consumers and political systems. The national data protection authorities and other national security are often not competent to address such large-scale negotiations and crises. This opens up the possibility of good reception of the European assistance with cyber security problems which relate to the private market and which overwhelm the national cyber defense systems. The aforementioned impact of contribution imbalance on the equal access to the ESM is another argument for pursuing a joint hybrid cyber security strategy.

Conclusions

The push towards uniformity in the policies and standards concerning cyber security across the EU is consistent with the trend of Europeanization of wider security policy. Following Ladrech, Gross[28]

[28] E. Gross, *Germany and European security and defence cooperation: The Europeanization of national crisis management policies?*, "Security Dialogue", no. 38(4)/2007, p. 504; R. Ladrech, *Europeanization of domestic politics and institutions: The case of France*, "Journal of Common Market Studies", no. 32(1)/1994, p. 69.

defines Europeanization of security policy in terms of the influence of European cooperation on nation states as 'incremental process reorienting the direction and shape of policies to the degree that European cooperation political and economic dynamics become part of the organizational logic of national politics and policy making'. This definition is consistent with the nation state sovereignty as far as the process of reorienting the domestic policies may be initiated by domestic decisions. Thus understood Europeanization invites a bottom-up counter-process, which consists in 'the emergence and development at the European level of distinctive structures of governance'.[29]

In the recent years the EU has taken steps towards facilitating the bottom-up integration of cyber security policies, most notably through building the foundations of the future contractual partnership between the private and public sector.[30] This step closely resembles the German initiative of private-public partnership in the CERT Alliance and opens a possibility of trust-building activity within the private and public sectors of the member states. With further consideration of the three principles of cooperation and their extension onto the cyber security strategies across the EU, the member states may join their cyber security efforts to the level which is under their control, and therefore, preserving their state sovereignty in decision-making, and to the long-term advantage of each member, where the payoff is bound to manifest itself either through enhanced protection of critical infrastructure or through improved conditions of participation in the ESM.

The author argued that the EU member states should pursue a joint strategy of cyber security and cyber defense. This claim does not immediately imply support for the current EU legislation, in particular for enforcing the NIS Directive or the operation of ENISA in its currently planned capacity. Three principles of European cooperation were discussed and followed by a proposal to center the joint strategic effort around promoting and explicating the practical and procedural consequences of these principles.

The first principle, called the principle of efficiency in European cooperation, states that sharing the costs of building a resilient cyber security system is beneficial, assuming that a perceivably fair distribution of commitments is agreed upon. The principle of non-aggression between

[29] T. Risse, M. Green Cowles, J. Caporaso, *Europeanization and Domestic Change: Introduction*, in: *Transforming Europe: Europeanization and Domestic Change*, eds. M. Green Cowles, J. Caporaso, T. Risse, Cornell University Press, Ithaca, NY 2001, p. 3.

[30] C. Banasiński, *Cyberbezpieczeństwo. Zarys wykładu (Cybersecurity. Draft of the lecture)*, Warszawa 2018, pp. 55–56.

the member states, which is fundamental to the European project as a whole, requires extending onto the new realms of warfare, including cyber warfare. Finally, the principle of priority of the ESM states that equal participation in the ESM be seen as an objective by the member states without being taken for granted. The consequence of this change is that the member states negotiate their respective contributions to cyber security systems and tools instead of relying on the EU regulations which guarantee a certain level of ESM access.

All in all, a bottom-up approach to joining and uniformization of European cyber defense is argued for. This approach requires that the European cyber security agencies, including ENISA, focus their efforts of addressing the trust deficit among the member states through facilitating the environment for safe information exchange, instead of communicating with the member states through the medium of regulations and prescribing security standards. More generally, the author postulates that the European authorities embrace the inherent political character of international trust-building and aspire to the role of mediator, as opposed to presenting themselves as apolitical agents focused on purely technical aspects of European cyber security.

References

Baezner M., Robin, P., *Cyber-conflict between the United States of America and Russia* (No. 2), ETH Zurich, 2017.

Banasiński C., *Cyberbezpieczeństwo. Zarys wykładu (Cybersecurity. Draft of the lecture)*, Warszawa 2018.

Brun L., *The role of the European Union Agency for Network and Information Security (ENISA) in the governance strategies of European cybersecurity*, Faculté des sciences économiques, sociales, politiques et de communication, Université catholique de Louvain, Bellanova, Rocco 2018.

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, Brussels, 06.07.2016.

Ghafur S., Kristensen S., Honeyford K., Martin G., Darzi A., Aylin P., *A retrospective impact analysis of the WannaCry cyberattack on the NHS*, "NPJ digital medicine", no. 2(1)/2019, DOI: https://doi.org/10.1038/s41746-019-0161-6

Global intelligence oversight: governing security in the twenty-first century, eds. Z. Goldman, S. Rascoff, Oxford University Press, Oxford 2016.

Greenberg A., *The untold story of NotPetya, the most devastating cyberattack in history*, "Wired", August 22, 2018.

Gross E., *Germany and European security and defence cooperation: The Europeanization of national crisis management policies*, "Security Dialogue", no. 38(4)/2007.

Hassner P., *An overview of the problem*, in: *War and Peace: European Conflict Prevention*, Chaillot Paper 11, Institute for Security Studies of WEU, 1993.

https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework (access 10.01.2020).

https://ec.europa.eu/digital-single-market/en/implementation-nis-directive-germany (access 2505. 2018).

https://ec.europa.eu/growth/single-market_en (access 10.01.2020).

https://eeas.europa.eu/headquarters/headquarters-homepage/63376/stronger-eu-defence-face-global-challenges_en (access 10.12.2019).

https://en.oxforddictionaries.com/definition/us/cyberthreat (access 25.05.2018).

https://www.cert-verbund.de/ (access 25.05.2018).

https://www.cybereason.com/blog/how-geopolitical-events-will-change-cybersecurity-in-2020 (access 30.12.2019).

https://www.eu2017.ee/videos/eu-cyber-security-conference-arne-schonbohm-and-guillaume-poupard.html (access 25.05.2018).

https://euobserver.com/justice/141860 (access 10.03.2020).

https://www.euractiv.com/section/cybersecurity/interview/commission-should-walk-the-walk-on-cybersecurity-german-chief-says/ (access 25.05.2018).

https://www.euractiv.com/section/cybersecurity/news/ansip-vows-to-respect-sovereignty-with-new-cybersecurity-measures/ (access 25.05.2018).

https://www.euractiv.com/section/cybersecurity/news/europe-needs-digital-border-controls-industry-chief-says/ (access 3.03.2020).

https://www.euractiv.com/section/cybersecurity/news/juncker-announces-massive-cyber-security-overhaul/ (access 10.03.2020).

https://www.secureworks.com/blog/cyber-threat-basics (access 25.05.2018).

Ladrech R., *Europeanization of domestic politics and institutions: The case of France*, "Journal of Common Market Studies", no. 32(1)/1994, DOI: https://doi.org/10.1111/j.1468-5965.1994.tb00485.x.

Nakashima E., *Russian military was behind NotPetya cyberattack in Ukraine, CIA concludes*. "The Washington Post", no. 12/2018.

Newman S., *Surviving ransom driven DDoS extortion campaigns*, "Cyber Security: A Peer-Reviewed Journal", no. 3(1)/2019.

Obermayer B., Obermaier F., *The Panama Papers: Breaking the story of how the rich and powerful hide their money*, Oneworld Publications 2016.

Risse T., Green Cowles M., Caporaso J., *Europeanization and Domestic Change: Introduction*, in: *Transforming Europe: Europeanization and Domestic Change*, eds. M. Green Cowles, J. Caporaso, T. Risse, Cornell University Press, Ithaca, NY 2001.

Sliwinski K., *Moving beyond the European Union's weakness as a cyber-security agent*, "Contemporary Security Policy", no. 35(3)/2014, DOI: https://doi.org/10.1080/13523260.2014.959261.

The joint communication to the European Parliament and the European Council of the European Commission's High Representative of the Union for Foreign Affairs and Security Policy "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", JOIN(2017) 450 final, Brussels, 13.09.2017.

Von Solms R., Van Niekerk J., *From information security to cyber security*, "Computers & Security", no. (38)/2013, DOI: https://doi.org/10.1016/j.cose.2013.04.004.

Welchman G., *The Hut Six Story: Breaking the Enigma Codes*, M&M Baldwin 1997.

Wouters J., Naert F., *The European Union and Conflict Prevention: a Brief Historic Overview*, "KULeuven Institut of International Law Working Paper", no. 52, April 2003, DOI: https://doi.org/10.1007/978-90-6704-539-1_3.